The Internet

How has it affected our Privacy & Freedom of Information

This reports aims to detail the group findings on our chosen topic and also a brief conclusion on the matter

2nd Year

Lecturer: Annette Cosgrove

*Group Members:*

Diane Long

Daniel Phillips

Elizabeth O’Callaghan

Table of Contents

[**Introduction** 3](#_Toc320019967)

[**What is Internet Privacy?** 3](#_Toc320019968)

[E-mail accounts 3](#_Toc320019969)

[Social Media Websites 3](#_Toc320019970)

[Online Banking Websites 3](#_Toc320019971)

[Online Shopping Websites e.g. EBay 4](#_Toc320019972)

[Consequences of entering this information 4](#_Toc320019973)

[When looking for employment in the future 4](#_Toc320019974)

[**Hacking** 5](#_Toc320019975)

[First Hacks 5](#_Toc320019976)

[The Golden Era 5](#_Toc320019977)

[The Split Forms 6](#_Toc320019978)

[Criminalisation 6](#_Toc320019979)

[Hackers – Good & Bad 6](#_Toc320019980)

[The Newest Frontier 6](#_Toc320019981)

[**Freedom of Information** 7](#_Toc320019982)

[The pros of censorship 7](#_Toc320019983)

[Religious Conflict 7](#_Toc320019984)

[Political Propaganda 7](#_Toc320019985)

[Terrorism 7](#_Toc320019986)

[Unwelcome Attention 7](#_Toc320019987)

[What are the cons of censorship? 8](#_Toc320019988)

[Freedom of Media 8](#_Toc320019989)

[Government Censorship 8](#_Toc320019990)

[Freedom of Choice 8](#_Toc320019991)

[Freedom of Creativity 8](#_Toc320019992)

[Public has the right to know 8](#_Toc320019993)

[**Conclusion** 8](#_Toc320019994)

# Introduction

The purpose of the report is to create a presentation of facts and findings about how that Internet has affected our privacy and freedom of information. By examining a range of on-line articles and internet sites on the topic, we hope to highlight the advantages and disadvantage we all face with regard to the issue. We decided to approach researching this by investigating a couple of different angles, the first being the aspect of on-line privacy, what this means and how it affects us all. We will then discuss the growing and ever present danger of computer hacking, looking into the background of this topic and the implications of computer hacking. This will finally lead our research onto the freedom of information on the Internet, investigating web censorship in particular.

# What is Internet Privacy?

Internet privacy involves the right or mandate of personal privacy concerning the storing, repurposing, providing to third-parties, and displaying of information pertaining to oneself via the Internet. This information can include pictures, bank account details, e-mail address' etc. Anything personal that you would not like other people knowing, is supposed to be kept private

**What websites require you to enter personal information?**

## E-mail accounts

In order to set up an e-mail account and have an e-mail address, you are required to enter certain information over the internet. Such information includes your name, address, a selected password to gain access to your account and a selected e-mail address to use.

## Social Media Websites

In order to join some of the social media websites such as Facebook or Twitter, you have to enter your e-mail address and select a password. Then you can add optional information if you wish such as a profile picture, your home address and contact information. Many adults do not share their home address or contact information but results show that many teenagers and younger children don’t see the harm in sharing this information. You can also add other types of information onto these such as pictures from family or social events, and you can have conversations with your friends in which every other person can view if certain privacy settings are activated.

## Online Banking Websites

The introduction of the facility of online banking has certainly made it more convenient to people to view their bank accounts as it means you don’t have to travel to a bank branch to get a statement, as you can log in to your bank account online and view it on the computer screen. But there is obviously many risks to this as hackers could get into your account and view all your information. In order to set up an online banking account you have to input lots of personal information including your bank account number and home address. Banks re assure users that people can not break into your online account but for some people it is too risky to use.

## Online Shopping Websites e.g. EBay

Another type of website that requires personal information is an online shopping website, for example EBay. EBay requires an account in your name to be set up in order for you to buy goods over the internet. Your account information consists of your name, home address and credit card information. This information cannot be displayed to every other user of EBay but the information is still out there and hackers can track it down.

## Consequences of entering this information

### When looking for employment in the future

It can be assumed these days that with the boom of social media websites, most people have an account with one of them whether its facebook, twitter or one of the other ones lesser known ones. Whether they use it on a day-to-day basis or never use it at all. This means that if you apply for a job, an employer can go on to one of the social media sites and browse around to see if you have a profile and the information that is displayed on these profiles whether its unsuitable conversations with a friend or a member of your family, to pictures that can be viewed of you when you were on a night out with your friends or another social event can be the difference to whether you get the job or not. This means that if you do have a profile on one of these sites, to make sure that there is nothing unsuitable on it that you would not want people seeing. This also suggests that with the boom in the use of the internet over the last decade or so, personal privacy is a thing of the past.

Privacy measures are provided on several social networking sites to try to provide their users with protection for their personal information. On Facebook for example privacy settings are available for all registered users. The settings available on Facebook include the ability to block certain individuals from seeing your profile, the ability to choose your "friends," and the ability to limit who has access to your pictures and videos. Privacy settings are also available on other social networking sites such as E-harmony and MySpace. It is the user's prerogative to apply such settings when providing personal information on the internet.

In late 2007 Facebook launched the Beacon program where user rental records were released on the public for friends to see. Many people were enraged by this breach in privacy.

Since the year 2000, Internet access worldwide has steadily been increasing. 92.8% of children between ages 12 and 18 report having access to Internet at home and 56% of these teenagers access this Internet alone in their room. The increase in Internet access for teenagers in a separate room or bedroom presents a concern of safety as their use of the Internet becomes unrestricted.

The risks that can be encountered through the usage of the Internet include issues of privacy. Children are more likely to disperse personal information to others across the Internet. 70% of children saw no problem in giving someone their home address or email. 12.7% of 10-12 year olds report sending pictures to others across the Internet.

Children and adolescents are very susceptible to misusing the Internet and ultimately risking their privacy. There is a growing concern among parents whose children are now starting to use Facebook and other social media sites on a daily basis. Website information collection practices is another growing concern as young individuals are more vulnerable and unaware of the fact that all of their information and browsing can and may be tracked while visiting a particular site.

Individuals who use the Internet have to realize that they must play a role in protecting their own privacy. They must be informed about all of the risks involved while surfing the Internet and browsing. For example, if on Twitter, threats include shortened links that lead you to potentially harmful places.

When you are in your e-mail inbox threats include email scams and attachments that get you to install malware and give up personal info. If on Torrent sites the threat includes malware hiding in video, music, and software downloads, and even while using your Smartphone threats include geolocation, meaning that your phone can detect where you are and post it online for all to see.

Certain measures that consumers are called to act upon include: updating virus protection, mind security settings, download patches, install firewalls, screen e-mail, shut down spyware, control cookies, deploy encryption, fend off browser hijackers, and block all pop-ups.

# Hacking

The right toprivacy in Internet activity is a serious issue facing society. Some users of the 'net wish to shieldtheir identities while participating in frank discussionsof sensitive topics. Others fulfil fantasies and harmlessly role play under the cover of a false identity in chartrooms, but there are the eternal ‘bad apples’ on the Internet, they are the people who useanonymous servers as more than a way to avoid responsibility for controversial remarks. Though it wasn’t yet called hacking, the earliest known incidents of modern technological mischief date from 1878 and the early days of the Bell Telephone Company. Teenage boys hired by Bell as switchboard operators intentionally misdirected and disconnected telephone calls, eavesdropped on conversations, and played a variety of other pranks on unsuspecting customers.

## First Hacks

The first bona fide appearance of a computer hacker occurs in the1960s. The term originated with model train enthusiasts who hacked their train sets in order to modify how they worked. Several of these same model train hackers later applied their curiosity and resourcefulness to the then new computer systems being deployed on the campus.

These and other early computer hackers were devout programming enthusiasts, experts primarily interested in modifying programs to optimize them, customize them for specific applications, or just for the fun of learning how things worked. The 1970s produced another type of hacker, one focused on telephone systems. Known as phreakers, these hackers discovered and exploited operational characteristics of the newly. All-electronic telephone switching network that enabled them to make long distance calls free of charge.

## The Golden Era

Hacking enjoyed a golden era of sorts in the 1980s. The introduction of turnkey personal computers are a turning point in hacker history. Now computers were no longer limited to the realms of hardcore hobbyists and business users -anyone, including existing and yet-to-be-realized hackers, could acquire a computer for their own purposes. Modems, devices that enabled computers to communicate with each other over telephone lines, were also more widely available and significantly extended the hacker’s reach.

## The Split Forms

Although hacking expanded and enjoyed glorification during its golden years, a divide was forming within the hacking community by the late 1980s. An increasing number of hackers were no longer satisfied with benign exploration of systems merely to learn how they worked. The hacker principle of freedom of technology was changing, and a younger generation interested in individual gain emerged. This new breed of “hacker” directed its knowledge and tenacity toward distinctly criminal pursuits, including the distribution of pirated commercial software, games, and viruses and worms that could virtually shut down systems.

The dark side fragmented even further as several groups formed electronic gangs driven to tap into the sensitive information housed within large institutions, like government and educational research centres. As happens with conventional street gangs, it didn’t take long for these groups to begin fighting each other, and the early 1990s saw an escalation of infighting that jammed phone lines and networks, and ultimately led to the demise and criminal prosecution of several groups.

## Criminalisation

Legislators and law enforcement began to get serious about criminalizing and prosecuting these activities in the mid-1980s. Governments passed its first hacking-related legislation, then in 1986. The act made computer tampering a crime punishable by significant jail time and monetary fines

## Hackers – Good & Bad

Although the term “hacker” is in widespread use, the sense in which it is employed is generally incorrect. Popular media and entertainment providers have long used it to describe anyone who tampers with a system, particularly in connection to criminal activity. This journalistic misuse of the name upset many traditional hackers, who responded to the vilification of their good name by offering a new term for these individuals: crackers. Crackers are vandals and thieves whose sole purpose is unauthorized cracking into secure systems for personal gain. This darker side of hacking has three main motivations with varying degrees of harm. The most benign cracks are attempts to gain unauthorized access in order to satisfy a personal motive such as curiosity or pride. The goal of the most serious and professional crackers is unauthorized access to systems or computer services in order to steal data for criminal purposes. For the cracker, everything is about *access* to information, especially if it is sensitive or protected. Moreover, crackers consider their illicit activities badges of honour to be worn with pride. Ironically, although most crackers are thought to live on the fringe of society, many have a tendency to downplay the consequences of their actions and generally rationalize their activities as being for the good of humanity.

## The Newest Frontier

One of the newest forms of hacking involves finding and connecting to unsecured Wireless Access Points (WAPs). Also called whacking, the practice has grown with the increasingly widespread use of wireless networks. Whacking capitalises on the relative ease with which many wireless networks can be accessed (generally because their owners haven’t taken steps to secure them). The wireless nature of these networks makes them easy to find and hack, and because they so often extend Internet access, wireless networks are especially enticing targets for unauthorized use.

# Freedom of Information

The area of greatest danger on the Internet is also its greatest feature, *free information*. The freedom of ideas and speech is something many people have died fighting for over the centuries and the notion that ideas and information should be controlled by governments or society as a whole, is very divisive one.

The motivations for censorship range from well-intentioned desires to protect children from unsuitable content to attempts to control a nation's access to information. No matter what the censors' reasons are, the end result is the same: *They block access to the* [*Web pages*](http://computer.howstuffworks.com/web-page.htm) *they identify as undesirable.*

For as long as there's been an Internet, China has sought to monitor and control how its citizens use it. That's no small task in the world's most populous country, which now has 485 million web-surfers. Technology known as ‘The Great Firewall’ blocks web sites on an array of sensitive topics (for example, democracy), while tens of thousands of government monitors and citizen volunteers regularly sweep through blogs, chat forums, and even e-mail to ensure nothing challenges the country's self-styled harmonious society. Together this massive network of Internet nannying is called ‘The Golden Shield Project’. Thousands of websites are blocked outright, and destinations such as YouTube, Flicker and Wikipedia are heavily restricted.

## The pros of censorship

Censorship controls the types of images and material that might be available to children, from pornography to violence, and whilst it is often extremely difficult to police what appears on the Internet, some level of censorship is essential to prevent the corruption of young and vulnerable minds.

### Religious Conflict

Censorship can help to prevent unnecessary religious conflict by avoiding a possible avenue for those trying to incite religious violence. Religious conflicts are avoided by the censorship of material deemed insulting or offensive to a particular religious community.

### Political Propaganda

Politically motivated propaganda is a dangerous tool for individuals and political figures to try and garner the support of the masses for their potentially dangerous ideas: censorship helps to prevent such ideas from finding a fertile breeding ground. It can be used to prevent politically motivated propaganda.

### Terrorism

Censoring sensitive information can stop unsuitable people gaining access to potentially harmful information. For example, Terrorists are prevented from learning about dangerous technology like the bomb making. And self harm websites.

### Unwelcome Attention

Censorship protects the privacy of certain individuals who might otherwise be subjected to unwelcome attention, such as public figures.

## What are the cons of censorship?

### Freedom of Media

Censorship stifles the freedom of the media and press, which is not in the spirit of democracy. Freedom of speech is compromised and it prevents the free flow of ideas.

### Government Censorship

Unscrupulous governments and individuals are apt to take advantage of censorship and use it to hide their own misdeeds from scrutiny of the world. Censorship has often been used by dictators to prevent the media reporting unsavory events in war torn and politically unstable countries. Religious fundamentalists like the Taliban use them to coerce the population. Government censorship has no place in a truly democratic society.

### Freedom of Choice

People should have the freedom to choose the type of information and ideas they wish to be exposed to rather than be told what they can and cannot do by a higher body. There can be different standards of morals among different societies quite different from the imposed ones by the censorship.

### Freedom of Creativity

Censorship not only stifles freedom of ideas, it also gags creativity. There are many ways that censors inhibit creativity, but some mediums that can be censored are books, films, music and military maps or certain areas on Google Maps.

### Public has the right to know

Censorship can be used to prevent the public finding out what immoral and illegal activities certain individuals have been up to in their private lives—information that the public has a right to know. Withholding of certain information will only leads to ignorance in society.

# Conclusion

We want to conclude by saying that in the years ahead, the Internet will have an even more profound effect on the way we work, live and learn. So as the Internet grows and evolves, we need to better understand and learn how best to protect ourselves online and become more aware of how to use the Internet safely. User-control and privacy concerns should be taken into account early in design processes—i.e. privacy-by-design. But there is significant risk that we will end up with a very effective distributed surveillance system, a dream come true for the metaphorical big brothers, electronic stalkers and cybercriminals. User-control and personal data protection have to be part of the design of the underlying infrastructure, the e-services that run on top of it, and the authority and management structure to run it.